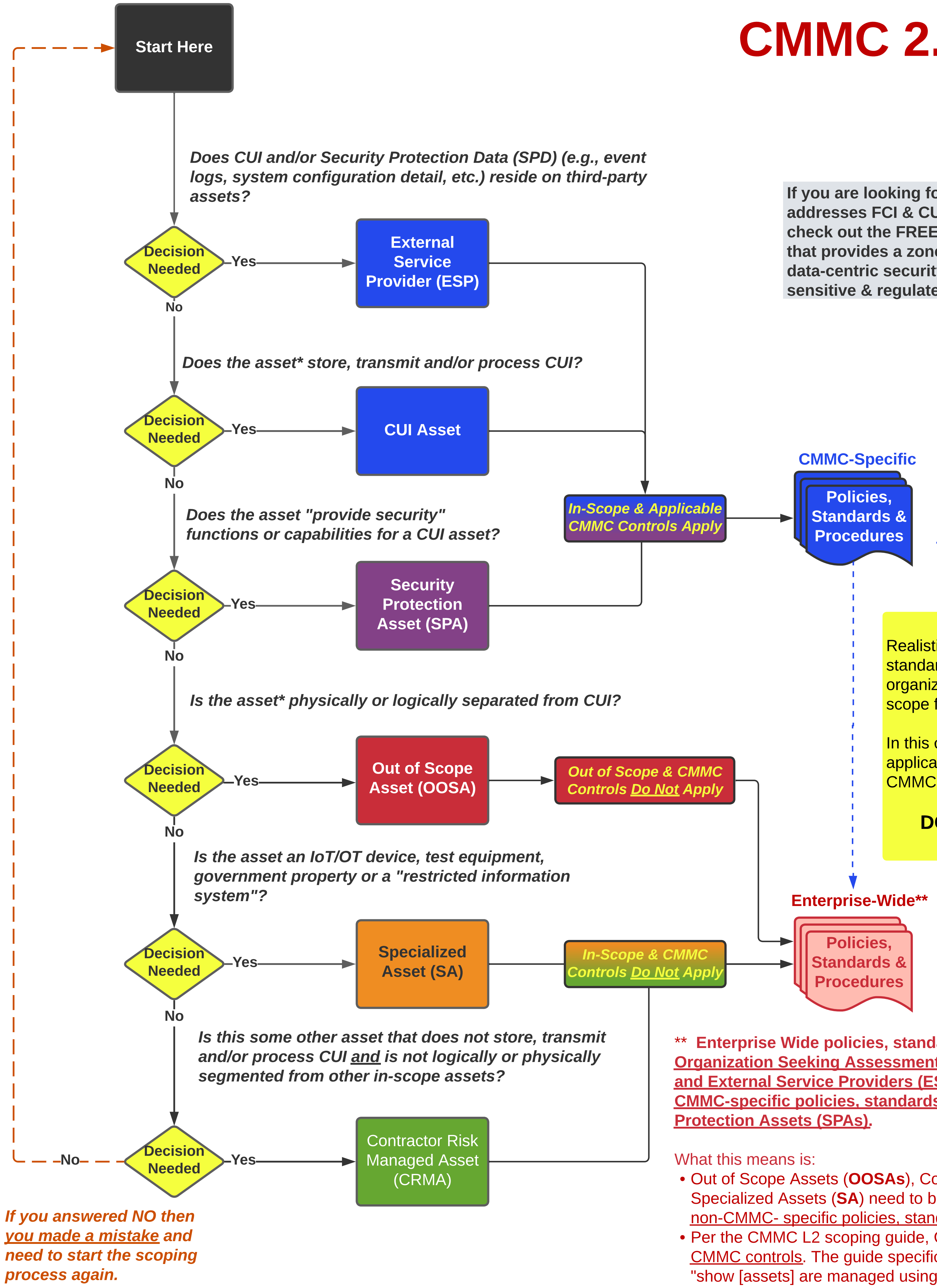
CMMC 2.0 Scoping Tree

version 2024.1



Start Here

Does CUI and/or Security Protection Data (SPD) (e.g., event logs, system configuration detail, etc.) reside on third-party assets?

Decision Needed — Yes → External Service Provider (ESP)

No

Does the asset store, transmit and/or process CUI?*

Decision Needed — Yes → CUI Asset

No

Does the asset "provide security" functions or capabilities for a CUI asset?

Decision Needed — Yes → Security Protection Asset (SPA)

In-Scope & Applicable CMMC Controls Apply

CMMC-Specific

Policies, Standards & Procedures

No

Is the asset physically or logically separated from CUI?*

Decision Needed — Yes → Out of Scope Asset (OOSA) → *Out of Scope & CMMC Controls Do Not Apply*

No

Is the asset an IoT/OT device, test equipment, government property or a "restricted information system"?

Decision Needed — Yes → Specialized Asset (SA) → *In-Scope & CMMC Controls Do Not Apply*

Enterprise-Wide**

Policies, Standards & Procedures

No

Is this some other asset that does not store, transmit and/or process CUI and is not logically or physically segmented from other in-scope assets?

Decision Needed — Yes → Contractor Risk Managed Asset (CRMA)

No

If you answered NO then you made a mistake and need to start the scoping process again.

If you are looking for a scoping guide that addresses FCI & CUI, but can do a lot more, then check out the FREE Unified Scoping Guide (USG) that provides a zone-based model to apply a data-centric security approach for scoping sensitive & regulated data

Unified Scoping Guide
Sensitive & Regulated Data
https://complianceforge.com/usg

CMMC AWESOMENESS!

www.CMMC-COA.com

CMMC-specific policies, standards and procedures are applicable to the system, application, service, person or External Service Provider (ESP).

Realistically, CMMC-specific documentation (e.g., policies, standards and procedures) should be a subset of the organization's overall Governance, Risk & Compliance (**GRC**) scope for policies, standards and procedures.

In this case, CMMC-specific requirements would only be applicable to those specific assets that require the use of CMMC controls to protect CUI

DOCUMENTATION: ENTERPRISE ≥ CMMC

🟦 CUI Asset
🟪 Security Protection Asset (**SPA**)
🟧 Specialized Asset (**SA**)
🟥 Out of Scope Asset (**OOSA**)
🟩 Contractor Risk Managed Asset (**CRMA**)

Process - CUI can be used by an asset (e.g., accessed, entered, edited, generated, manipulated or printed)

Store - CUI is inactive or at rest on an asset (e.g., located on electric media, in system component memory or in physical format such as paper documents).

Transmit - CUI is being transferred from one asset to another asset (e.g., data in transit using physical or digital transport methods).

** Enterprise Wide policies, standards and procedures are applicable to the Organization Seeking Assessment's systems, applications, services, people and External Service Providers (ESPs)) that are not specifically covered by CMMC-specific policies, standards and procedures for CUI Assets and Security Protection Assets (SPAs).

What this means is:

- Out of Scope Assets (**OOSAs**), Contractor Risk Managed Assets (**CRMA**) and Specialized Assets (**SA**) need to be appropriately governed by the organization's non-CMMC- specific policies, standards and procedures.
- Per the CMMC L2 scoping guide, CRMA and SA are in-scope, but not subject to CMMC controls. The guide specifically calls out that contractors are required to "show [assets] are managed using the contractor's risk- based security policies, procedures, and practices."

The Organization Seeking Assessment's non-CMMC specific policies, standards and procedures are applicable to governing those CRMA and SA, even though they are in-scope to CMMC. Enterprise-level policies, standards and procedures provide "reasonable security" for CRMAs and SAs, but not SPAs or CUI Assets.

*Definition: "asset" per CMMC Asset Scope - Level 2 guide

Asset Type	Security Protection Asset Examples
People	• Consultants who provide cybersecurity service • Managed service provider personnel who perform system maintenance • Enterprise network administrators
Technology	• Cloud-based security solutions • Hosted Virtual Private Network (VPN) services • SIEM solutions
Facility	• Co-located data centers • Security Operations Centers (SOCs) • Contractor office buildings